UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/750,430	12/31/2003	HongQian Karen Lu	76.0888	1787

41754 7590 06/28/2007	EXAMINER	
THE JANSSON FIRM	HOFFMAN, BRANDON S	
9501 N. CAPITAL OF TX HWY #202		
AUSTIN, TX 78759	ART UNIT	PAPER NUMBER
	2136	

MAIL DATE	DELIVERY MODE
06/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 December 2003*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some *   c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 are pending in this office action.

Specification

2. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. <u>Claims 1 and 17-20</u> are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

5. Claim 1 recites the limitation "a portable secure computing device" and "the secure computing device." There is insufficient antecedent basis for this limitation in the claim.

6. Claims 17-19 recite the limitation "the portable secure computing device." There is insufficient antecedent basis for this limitation in the claim.

7. Claim 20 is dependent upon claim 19 and therefore inherits its deficiencies.

Claim Rejections - 35 USC § 102

8.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9.   Claims 1-20 are rejected under 35 U.S.C. 102(b) as being anticipated by

Blatherwick et al. (U.S. Patent No. 6,269,395).

Regarding claim 1, Blatherwick et al. teaches a method for effecting secure

transactions over a computer network in a manner designed to foil identity theft

perpetrated from an untrusted computer, comprising:

- Connecting a client computer to the network wherein the client computer

  provides a user interface to interact with a user (col. 5, lines 66-67);

- Connecting a server computer to the network (col. 5, line 67 through col. 6, line

  2);

- Connecting a portable secure computing device to the network (fig. 1, ref. num

  11);

- Operating the secure computing device to communicate a list of available

  services to the client computer (fig. 3.1);

- Responsive to receiving the list of available services using the user interface to

  display the list of available services to a user (fig. 3.2.1);

- Responsive to a selection of one available service by the user, establishing a

    secure connection from the secure computing device to the server (fig. 12.1.2,

    ref. num 166);

- Securely communicating private information from the secure computing device to

    the server over the secure connection (fig. 12.1.2, ref. num 170).

Regarding claim 2, Blatherwick et al. teaches further comprising:

- Authenticating a user based on the private information (fig. 12.1.2, ref. num 170);

    and

- In response to successful authentication of the user, conducting a transaction

    between the client computer and the server computer (fig. 11, ref. num 143).

Regarding claim 3, Blatherwick et al. teaches further comprising transmitting from

the secure computing device to the server computer user identifying information (fig.

8.3, USER ID).

Regarding claim 4, Blatherwick et al. teaches wherein the user identifying

information includes a secret personal identification number (sPIN) (fig. 8.3,

PASSWORD).

Regarding claim 5, Blatherwick et al. teaches further comprising responsive to

receiving the user identifying information, operating the server computer to establish an

association among the user, the client and the secure computing device (fig. 12.1.2, ref. num 170).

Regarding <u>claim 6</u>, <u>Blatherwick et al.</u> teaches wherein the secure computing device has a personal identification number (PIN) wherein the sPIN and the PIN are unrelated (col. 6, lines 10-16).

Regarding <u>claim 7</u>, <u>Blatherwick et al.</u> teaches wherein the server computer uses the sPIN for only one session (fig. 8.3, password, the server does not store the PIN and therefore uses it for only one session).

Regarding <u>claim 8</u>, <u>Blatherwick et al.</u> teaches wherein the portable secure computing device is a smart card (fig. 3.3.1).

Regarding <u>claim 9</u>, <u>Blatherwick et al.</u> teaches a method for secure transactions over a computer network in a manner designed to foil identity theft perpetrated from an untrusted computer, comprising:

- Connecting a client computer to the network wherein the client computer provides a user interface to interact with a user (col. 5, lines 66-67);
- Connecting a server computer to the network (col. 5, line 67 through col. 6, line 2);
- Connecting a secure computing device to the network (fig. 1, ref. num 11);

- Establishing a secure connection from the secure computing device to the server (fig. 12.1.2, ref. num 166);

- Securely communicating private information from the secure computing device to the server over the secure connection (fig. 12.1.2, ref. num 170);

- Authenticating a user using the private information (fig. 12.1.2, ref. num 170); and

- In response to successfully authenticating the user, conducting a transaction between the client and the server (fig. 11, ref. num 143).

Regarding claim 10, Blatherwick et al. teaches wherein the step of securely communicating private information comprises pushing the private information from the secure computing device to the server computer (col. 15, lines 21-33).

Regarding claim 11, Blatherwick et al. teaches further comprising in response to successfully authenticating a user, operating the client to transmit an indication to the server that the secure computing device will send information necessary for a transaction; operating the server to wait for the information from the secure computing device; operating the client to select the information necessary for the transaction; and in response to selecting the information necessary for the transaction, operating the secure computing device to transmit the selected information securely to the server (fig. 12.1.2).

Regarding <u>claim 12</u>, <u>Blatherwick et al.</u> teaches wherein the step of securely communicating private information comprises operating the server computer to pull the private information from the secure computing device (col. 15, lines 21-33).

Regarding <u>claim 13</u>, <u>Blatherwick et al.</u> teaches further comprising: in response to successfully authenticating a user, operating the server to transmit a request to the secure computing device to provide information necessary to complete a transaction; in response to a request from the server for information necessary to complete a transaction, operating the secure computing device to notify the client that the server has made the request for information necessary to complete a transaction; in response to notification from the secure computing device that the server is requesting the information necessary to complete a transaction, operating the client to obtain a user's approval or denial of the request; and in response to a user's approval, transmitting the requested information from the secure computing device to the server in a secure manner (fig. 12.1.2).

Regarding <u>claim 14</u>, <u>Blatherwick et al.</u> teaches a system for effecting secure transactions over a computer network in a manner designed to foil identity theft through keystroke logging, comprising:

- A server computer connected to a computer network and operable to provide some form of online transactions (col. 5, line 67 through col. 6, line 2);

- A client computer connected to the computer network and operable to interface with a user (col. 5, lines 66-67);

- A secure computing device connected to the computer network and capable of establishing a secure connection with the server computer and the client computer (fig. 1, ref. num 11);

- Wherein the secure computing device has logic operable to store private user information (fig. 8.3); and

- Wherein the secure computing device has logic, in response to the initiation of a transaction between a user operating the client computer and the server computer, operable to securely transmit the private user information to the server computer in a manner such that only the server can interpret the private user information (fig. 12.1.2, ref. num 166 and 170).

Regarding claim 15, Blatherwick et al. teaches wherein the secure computing device has logic to transmit a map to the server computer, the map having the elements clientIP, cardIP, login credentials, and secret personal identification number (sPIN); wherein the server computer has logic to request a user to enter the sPIN and logic to verify that the entered sPIN matches the sPIN in the map (fig. 9.2).

Regarding claim 16, Blatherwick et al. teaches wherein the server computer has logic to destroy the map if the sPIN entered by the user does not match the sPIN of the map (14.2.2.1).

Regarding <u>claim 17</u>, <u>Blatherwick et al.</u> teaches wherein the portable secure computing device transmits the private user information upon a request by the user (fig. 12.1.2).

Regarding <u>claim 18</u>, <u>Blatherwick et al.</u> teaches wherein the portable secure computing device transmits the private user information upon a request by the server computer (fig. 12.1.2).

Regarding <u>claim 19</u>, <u>Blatherwick et al.</u> teaches wherein the portable secure computing device transmits the private user information to the server computer only upon permission granted by the user (fig. 8.3).

Regarding <u>claim 20</u>, <u>Blatherwick et al.</u> teaches wherein the server computer destroys the map in response to invalid sPIN, denial of permission from the user, and transaction completion (fig. 14.2.2.1).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Brandon Hoffman/

BH

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

6/23/07